UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ADRIANA WINKLER, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

LOUIS VUITTON NORTH AMERICA, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Adriana Winkler ("Winkler" or "Plaintiff") brings this Class Action Complaint, individually and on behalf of all others similarly situated ("Class Members") against Louis Vuitton North America, Inc. ("Louis Vuitton" or "Defendant") and allege as follows, based upon information and belief, the investigation of counsel, and the personal knowledge of Plaintiff.

NATURE OF THE CASE

1. This data breach class action involves the unauthorized access and exfiltration of sensitive Personal Identifiable Information (PII), including names, addresses, dates of birth, driver's license numbers, and/or partial Social Security numbers, of millions of Class Members, including Plaintiff.

2. Louis Vuitton is a high end online and brick-and mortal leather fashion design, manufacturing, and retail store.

3. The data breach described below occurred because Salesforce's Data Loader portal, used by Louis Vuitton to import or export customer data, is easily mimicked by bad actors.[1]

[1] *See* https://developer.Salesforce.com/tools/data-loader (last visited Jan. 13, 2026).

4. The data breach at issue was highly preventable and perpetrated using techniques and vulnerabilities known to Defendant well in advance.

5. On March 12, 2025, Salesforce published a blog for its customers titled "Protect Your Salesforce Environment from Social Engineering Threats."[2] Salesforce identified the specific type of voice phishing ("vishing") attack that would soon be used against Louis Vuitton and outlined five "proactive measures" Louis Vuitton should, and ultimately did not, take to strengthen its data security and access controls.[3]

6. On June 4, 2025, Google's Threat Intelligence Group ("GTIG") echoed Salesforce's own warnings when it reported that the cybercriminal organization UNC6240, a.k.a. ShinyHunters, was using a common and well-known social-engineering vishing technique to gain unauthorized access to Defendant's systems and databases because Defendant failed to implement fundamental and basic security measures that could have prevented the data breach.[4] GTIG explained that ShinyHunters was "*a financially motivated threat cluster that specializes in voice phishing (vishing) campaigns specifically designed to compromise organizations' Salesforce instances for large-scale data theft and subsequent extortion*."[5] GTIG highlighted that "it's essential for [Defendant] to configure and manage access, permissions, and user training according to best practices" to prevent such data security incidents.[6]

7. On or about July 2, 2025, Louis Vuitton discovered an unauthorized cyber-attack involving Salesforce's databases containing Louis Vuitton's customer information (the "Data

---

[2] *See* https://www.Salesforce.com/blog/protect-against-social-engineering/ (last visited Jan. 13, 2026).
[3] *Id.*
[4] *See* https://cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion (last visited Jan. 13, 2026).
[5] *Id.* (emphasis added).
[6] *Id.*

Breach").[7] According to Louis Vuitton, its forensic investigation revealed the unauthorized cyber incursion occurred on June 7, 2025.[8]

8. Plaintiff and Class Members have been substantially injured by Defendant's data security failures. Plaintiff further believes that hers and Class Members' PII has or will be published for sale on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

9. As a result of the Data Breach, Plaintiff has suffered numerous injuries, including invasion of privacy, lost time and expenses mitigating the risk of data misuse, diminishment in value of her PII, and failing to receive the benefit of the bargain reached with Defendant.

10. Plaintiff brings this action to hold Defendant accountable for its data security failures, enjoin its continued failure to implement basic and fundamental data security practices, and recover damages and all other relief available at law on behalf of themselves and members of the classes they seek to represent.

PARTIES

A. Defendant

11. Louis Vuitton is a high-end leather and fashion design and manufacturing company that is a subsidiary of LVMH Moët Hennessy Louis Vuitton with its North American headquarters and principal place of business at 1 East 57th Street, New York, New York 10022. Louis Vuitton is organized and incorporated under the laws of the State of New York.

---

[7] Louis Vuitton Data Breach Notice to South Carolina Attorney General, https://consumer.sc.gov/sites/consumer/files/Documents/Security%20Breach%20Notices/2025/Consumer%20Notice%20-%20Louis%20Vuitton%20North%20America%2C%20Inc.%20-%201.pdf (last visited Jan. 15, 2026).

[8] *Id.*

12. Louis Vuitton is a citizen of New York.

B. Plaintiff

13. Plaintiff Adriana Winkler is a resident of Anne Arundel County, Maryland and a Louis Vuitton customer.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than one hundred putative Class Members, and minimal diversity exists because many putative Class Members are citizens of a different state than any Defendant.

15. This Court has personal jurisdiction over Louis Vuitton because Louis Vuitton maintains its headquarters and principal places of business in this District. Louis Vuitton also conducts substantial business in this District, including operating at least seven brick and mortar locations in Manhattan, marketing to customers in this District and accepting and processing payments in this District, engages in the conduct at issue in this District, and/or otherwise has substantial contacts with this District and purposely avails itself of the Courts in this District.

16. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(1)–(2), 1391(b)(2), and 1391(c)(2) as Louis Vuitton's principal place of business is in this District, and a substantial part of the events giving rise to the claims emanate from activities within this District.

FACTUAL ALLEGATIONS

I. LOUIS VUITTON'S BUSINESS

17. Louis Vuitton, founded in 1854 in Paris, France, is a global high end fashion design and manufacturer specializing in leather goods, clothes, shoes, and handbags.[9]

18. Louis Vuitton is well aware of the necessity of data security for its customers and employees. Louis Vuitton's Privacy Policy provides that it "use[s] reasonable technical, administrative, and physical controls, procedures and practices to safeguard Personal Information" and "protect the Personal Information from unauthorized or illegal access, destruction, use, modification, and disclosure."[10]

19. Louis Vuitton receives the PII of individuals from its employees and the entities and individuals that use its services. In turn, Louis Vuitton entrusts this PII to its third-party vendors and service providers like Salesforce.

20. Louis Vuitton is a Salesforce customer. Louis Vuitton stores its employees' and customers' PII on Salesforce's cloud-based software, network, and/or products.

II. DEFENDANT OBTAINS, COLLECTS, USES, AND DERIVES A BENEFIT FROM THE PII OF PLAINTIFF AND CLASS MEMBERS.

21. Defendant obtains, collects, uses, and derives a benefit from Plaintiff's and Class Members' PII. Defendant uses this PII to provide goods, making a profit therefrom. Defendant would not be able to obtain revenue if not for the acceptance and use of this PII.

[9] https://www.lvmh.com/en/our-maisons/fashion-leather-good/louis-vuitton (last visited Jan. 15, 2026).

[10] https://us.louisvuitton.com/eng-us/legal-notices#privacy-policy (last visited Jan. 15, 2026).

22. By collecting Plaintiff's and the Class Members' PII, either directly or indirectly, Defendant assumed legal and equitable duties to Plaintiff and the Class Members to protect and safeguard their PII from unauthorized access and intrusion.

23. Defendant recognized this duty in its privacy policies and marketing to its customers and employees.

24. Defendant's assurances of maintaining high standards of cybersecurity demonstrate it recognizes it has a duty to use reasonable measures to protect the PII it collects and maintains.

25. Defendant violated its explicit privacy statements and failed to adopt reasonable and appropriate security practices and procedures, including administrative, physical security, and technical controls, to safeguard Plaintiff's and Class Members' PII.

26. As a result, Plaintiff's and Class Members' PII was accessed and stolen from Defendant's inadequately secured data systems in a massive and preventable Data Breach.

III. THE DATA BREACH.

27. On March 12, 2025, Salesforce published a blog on its website for its numerous customers titled "Protect Your Salesforce Environment from Social Engineering Threats."[11] The blog identified the precise scheme employed by ShinyHunters to perpetrate the Data Breach.

28. Specifically, Salesforce explained, "***Threat actors have been observed employing various social engineering tactics, including voice phishing (i.e., "vishing"), to impersonate members of an IT Support team over the phone. They have been reported luring our customers' employees and third-party support workers to phishing pages designed to steal credentials and MFA tokens or prompting users to navigate to the login.Salesforce[.]com/setup/connect page in***

[11] *See* https://www.Salesforce.com/blog/protect-against-social-engineering/ (last visited Jan. 13, 2026).

order to add a malicious connected app. In some cases, we have observed that the malicious connected app is a modified version of the Data Loader app published under a different name and/or branding. Once the threat actor gains access to a customer's Salesforce account or adds a connected app, they use the connected app to exfiltrate data."[12]

29. Salesforce identified five steps customers, including Louis Vuitton, should take to fortify their networks and systems from this precise vishing attack: (1) restrict network access through IP addresses and login ranges to customers' enterprise and VPN network; (2) implement the principle of least privilege and "Grant users only the permissions they need to do their jobs — no more, no less"; (3) enable multi-factor authentication because "***MFA adds an extra layer of defense, particularly against phishing attacks*** . . . ."; (4) use the suite of security tools available in Salesforce Shield; and (5) add a security point of contact "To ensure that we can reach your organization in the case of a security event . . . ."[13]

30. Two months later, in and around May 2025, notorious cybercriminal group ShinyHunters reportedly began a prolonged and devastating cyber-attack on Salesforce and Salesforce's customers, including Louis Vuitton.

31. By June 4, 2025, GTIG outlined the common and well-known social-engineering "voice phishing" techniques ShinyHunters was using to gain unauthorized access to Defendant's systems and databases.[14] GTIG highlighted that "it's essential for [Defendant] to configure and manage access, permissions, and user training according to best practices" in order to prevent such data security incidents.[15] GTIG specifically warned that "ShinyHunters extortion group [was]

[12] *Id.* (emphasis added).
[13] *Id.* (emphasis added).
[14] *See* https://cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion (last visited Jan. 13, 2026).
[15] *Id.*

conducting social engineering attacks against multi-national companies to steal data from organizations' Salesforce platforms."[16] And that "The extortion involves calls or emails to employees of the victim organization demanding payment in bitcoin within 72 hours."[17]

32. GTIG laid out the vishing scheme being used in painstaking detail: "UNC6040 has demonstrated repeated success in breaching networks by having its operators impersonate IT support personnel in convincing telephone-based social engineering engagements. This approach has proven particularly effective in tricking employees, often within English-speaking branches of multinational corporations, into actions that grant the attackers access or lead to the sharing of sensitive credentials, ultimately facilitating the theft of organization's Salesforce data."[18] GTIG further explained that "A prevalent tactic in UNC6040's operations involves deceiving victims into authorizing a malicious connected app to their organization's Salesforce portal. This application is often a modified version of Salesforce's Data Loader . . . ."[19]

33. GTIG connected the dots back to Salesforce's blog post explaining that "During a vishing call, the actor guides the victim to visit Salesforce's connected app setup page to approve a version of the Data Loader app with a name or branding that differs from the legitimate version. This step inadvertently grants UNC6040 significant capabilities to access, query, and exfiltrate sensitive information directly from the compromised Salesforce customer environments. ***This methodology of abusing Data Loader functionalities via malicious connected apps is consistent with recent observations detailed by Salesforce in their guidance on protecting***

[16] *See* https://www.bleepingcomputer.com/news/security/google-hackers-target-Salesforce-accounts-in-data-extortion-attacks/ (last visited Jan. 13, 2026).
[17] *See* https://cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion (last visited Jan. 14, 2026).
[18] *Id.*
[19] *Id.*

Salesforce environments from such threats."[20] GTIG expressly warned that ShinyHunters' attacks were targeting large companies that already used a Salesforce cloud-based CRM platform—exactly the type of platform used by Defendant.[21] GTIG explained that ShinyHunters "may be preparing to escalate their extortion tactics by launching a data leak site (DLS). These new tactics are likely intended to increase pressure on victims . . . ."[22] GTIG warned that ShinyHunters' lateral movement through Defendant's systems was not limited to Salesforce environments explaining that "Upon obtaining access, UNC6040 has been observed immediately exfiltrating data from the victim's Salesforce environment using Salesforce's Data Loader application. Following this initial data theft, ***UNC6040 was observed leveraging end-user credentials obtained through credential harvesting or vishing to move laterally through victim networks, accessing and exfiltrating data from the victim's accounts on other cloud platforms such as Okta and Microsoft 365***."[23] GITG identified almost identical steps as those identified by Salesforce that corporations that used Salesforce should implement to mitigate against this particular ShinyHunters threat.[24] Despite GTIG's and Salesforce's extensive and express warnings, Louis Vuitton failed to take appropriate steps to prevent the unauthorized access.

34. The Data Breach occurred on June 7, 2025.[25] Louis Vuitton claims it did not become aware of the Data Breach until roughly a month later, on July 2, 2025 – which is in and of

[20] *Id.* (emphasis added).
[21] *Id.*
[22] *Id.*
[23] *Id.* (emphasis added).
[24] *Id.*
[25] Louis Vuitton Data Breach Notice to South Carolina Attorney General, https://consumer.sc.gov/sites/consumer/files/Documents/Security%20Breach%20Notices/2025/Consumer%20Notice%20-%20Louis%20Vuitton%20North%20America%2C%20Inc.%20-%201.pdf (last visited Jan. 15, 2026).

itself troubling with respect to Louis Vuitton's data security practices.[26] Louis Vuitton's Data Breach Notice advised customers that their names, contact information, addresses, dates of birth, passport numbers, and government ID numbers were exposed in the Data Breach.[27] Recognizing the imminent risk of identity theft and fraud, Louis Vuitton encouraged customers to remain vigilant in looking for suspicious activity and offered affected customers credit monitoring and identity theft protection.[28]

35. Despite becoming aware of the Louis Vuitton Data Breach, on July 2, 2025, Louis Vuitton did not begin notifying affected American customers until August 22, 2025.[29]

36. Defendant failed to take the necessary precautions to safeguard and protect Plaintiff's and Class Members' PII from unauthorized access and exploitation. The risk of cyberattacks, such as the one that occurred here, were or should have been well-known to Defendant. Defendant could have taken, but did not take, numerous simple measures to prevent the Data Breach. Defendant's actions and inactions represent a flagrant disregard of the rights of Plaintiff and the Class Members.

IV. RELEVANT INDUSTRY STANDARDS AND REGULATIONS FOR DATA SECURITY

A. United States Federal Trade Commission Guidelines

37. The United States Federal Trade Commission ("FTC") has issued numerous forms of guidance and taken enforcement actions that outline the data security industry standards applicable to Defendant.

[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*

38. For example, the FTC's enforcement actions have established that a company's failure to maintain reasonable and appropriate data security of consumer PII violates the FTC Act's prohibition against "unfair or deceptive acts."[30]

39. In 2016, the FTC published guidance entitled *Protecting Personal Information: A Guide for Business* (the "FTC 2016 Guidance"). The FTC 2016 Guidance:

a. Stresses the importance of "[c]ontrol[ling] access to sensitive information" and expressly encourages businesses to "[c]onsider using multi-factor authentication, such as requiring the use of a password and a code sent by different methods."[31]

b. Emphasizes that companies should respond appropriately when credentials are compromised, providing that businesses should "[r]equire password changes when appropriate—for example, following a breach."

c. Instructs companies to restrict data access privileges by "[s]cal[ing] down access to data" and ensuring that "each employee should have access only to those resources needed to do their particular job."[32]

d. Warns companies that their data security practices depend on their personnel, which "includ[e] contractors" and encourages companies to "investigate [contractor] data security practices and compare their standards" and "verify compliance" with written security expectations.

e. Recommends that companies encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems and respond to security incidents.

f. Advises companies not to maintain PI longer than necessary, not to collect more PI than necessary, to use industry-tested methods for data security, and monitor and respond to suspicious activity.

40. In 2021, the FTC amended its "Safeguards Rule" that applies to financial institutions, including retailers that issue their own credit cards to consumers and companies that

[30] *See, e.g.*, *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020) (citing *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015)).
[31] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 14, 2026).
[32] *Id.*

bring together buyers and sellers of products and services.[33] The Safeguard Rule expressly requires covered businesses to "[i]mplement multi-factor authentication ["MFA"] for anyone accessing customer information on [the business's] system," to "[i]mplement and periodically review access controls [to] [d]etermine who has access to customer information and reconsider on a regular basis whether they still have a legitimate business need for it," and to "[i]mplement procedures and controls to monitor when authorized users are accessing customer information on your system and detect unauthorized access."[34]

41. In February 2023, the FTC published an article entitled *Security Principles: Addressing underlying causes of risk in complex systems.* The article highlighted the importance of MFA, stating that it "is widely regarded as a critical security practice because it means a compromised password alone is not enough to take over someone's account."[35]

B. Data Breaches Are Preventable

42. Despite the growing body of publicly available information regarding the rise of ransomware attacks, vishing schemes, and other forms of cyberattacks that compromise PII, Defendant's approach to maintaining the privacy of Plaintiff's and Class Members' PII was inadequate, unreasonable, negligent, and reckless. Defendant failed to use reasonable security procedures and practices appropriate to the nature of the sensitive information Defendant was maintaining and transferring for Plaintiff and Class Members such as encrypting the information or deleting it when no longer needed, limiting employee access keys to PII, and adequately training

[33] 16 C.F.R. §§ 314.2(h)(2)(i), (xiii).
[34] *See* https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last visited Jan. 13, 2026).
[35] *See* https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems (last visited Jan. 13, 2026).

its employees concerning vishing attacks and other social engineering schemes, which caused the exposure of Plaintiff's and Class Members' PII.

43. As explained by the FBI, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[36]

44. Defendant could have prevented this Data Breach. It could have and should have implemented measures—as recommended by the U.S. Government—to prevent and detect cyberattacks and/or ransomware attacks, including, but not limited to, the following:

- **Implement an awareness and training program**. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- **Enable strong spam filters** to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- **Scan all incoming and outgoing emails** to detect threats and filter executable files from reaching end users.
- **Configure firewalls** to block access to known malicious IP addresses.
- **Patch operating systems, software, and firmware on devices**. Consider using a centralized patch management system.
- **Set anti-virus and anti-malware programs to conduct regular scans automatically**. Ensure these programs run automatic scans to detect and remove potential threats.
- **Manage the use of privileged accounts based on the principle of least privilege**: no users should be assigned administrative access unless absolutely needed; and those

[36] Ransomware Prevention and Response, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Jan. 13, 2026).

with a need for administrator accounts should only use them when necessary.

- **Configure access controls**—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- **Disable macro scripts from office files transmitted via email**. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- **Implement Software Restriction Policies (SRP)** or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- **Disable Remote Desktop protocol (RDP)** if it is not being used.

- **Use application whitelisting**, which only allows systems to execute programs known and permitted by security policy.

- **Execute operating system environments or specific programs in a virtualized environment**. Run sensitive systems or programs in isolated virtual environments to reduce risk.

- **Categorize data based on organizational value** and implement physical and logical separation of networks and data for different organizational units.[37]

45. To prevent and detect cyberattacks and ransomware attacks, Defendant could and should have implemented the following preventive measures, as recommended by Microsoft's Threat Protection Intelligence Team:

- **Secure internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management

[37] *Id.*

- Perform regular audits
- Remove privileged credentials

- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise

- **Include IT Pros in security discussions**
  - Ensure collaboration among security operations, security admins, and information technology admins to configure servers and other endpoints securely

- **Build credential hygiene**
  - Use multifactor authentication or network level authentication and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and Antimalware Scan Interface for Office Visual Basic for Applications.[38]

46. Similarly, Defendant could and should have implemented measures—also recommended by the U.S. Government—to prevent and detect cyberattacks and/or ransomware attacks, including the following recommendations:

- Know what personal information you have in your files and on your computers.

- Keep only what you need for your business.

- Protect the information that you keep.

[38] *See* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Jan. 13, 2026).

- Properly dispose of information you no longer need. Create a plan to respond to security incidents.[39]

47. Finally, Defendant could and should have implemented the following measures—also recommended by the U.S. Government—to prevent and detect cyberattacks and/or ransomware attacks, including the following recommendations:

- **Conduct regular vulnerability scanning to identify and address vulnerabilities**, especially those on internet-facing devices, to limit the attack surface.

- **Regularly patch and update software and operating systems to the latest available versions.** Prioritize timely patching of internet-facing servers that operate software for processing internet data such as web browsers, browser plugins, and document readers-especially for known exploited vulnerabilities….

- **Limit the use of RDP and other remote desktop services.** If RDP is necessary, apply best practices. Threat actors often gain initial access to a network through exposed and poorly secured remote services, and later traverse the network using the native Windows RDP client.

- **Ensure all on-premises, cloud services, mobile, and personal devices are properly configured and security features are enabled.** For example, disable ports and protocols not being used for business purposes.[40]

48. Because Defendant was collecting, storing, and transferring highly sensitive PII belonging to Plaintiff and Class Members, it could—and should—have implemented all of the above measures to prevent and detect cyberattacks.

49. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks or vishing attacks, resulting

[39] *See* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Jan. 13, 2026).
[40] *See* https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf (last visited Jan. 14, 2026).

in the Data Breach and data thieves accessing and acquiring the PII of Plaintiff and millions of Class Members.

C. Industry Standards Specific to Cloud Data Storage

50. In addition to the general data security standards described above, numerous authorities have issued guidance specific to cloud data storage, defining the roles and responsibilities of cloud service customers (like Louis Vuitton).

i. Governmental Authorities

51. In June 2020, the FTC published an article titled, *Six steps toward more secure cloud computing.* The article warned, "As cloud computing has become business as usual for many businesses, frequent news reports about data breaches and other missteps should make companies think carefully about how they secure their data." The article expressly highlighted the importance of MFA in protecting consumer data stored on cloud services, recommending businesses: "Require multi-factor authentication and strong passwords to protect against the risk of unauthorized access."[41]

52. In March 2023, the FTC issued a Request for Information seeking public comment on "Business Practices of Cloud Computing Providers that Could Impact Competition and Data Security."[42] After reviewing over 100 public comments on the issue, the FTC published a report in November 2023 titled, *Cloud Computing RFI: What we heard and learned.* The report expressly flagged the room for improvement in cloud security as follows: "[A] a number of commenters argued there is a great deal of room for improvement in cloud security; that default security

[41] https://www.ftc.gov/business-guidance/blog/2020/06/six-steps-toward-more-secure-cloud-computing (last visited Jan. 13, 2026).
[42] https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-seeks-comment-business-practices-cloud-computing-providers-could-impact-competition-data (last visited Jan. 13, 2026).

configurations could be better; and that the "shared responsibility" model for cloud security often lacks clarity, which can lead to situations where neither the cloud provider nor the cloud customer implements necessary safeguards."[43]

53. In March 2024, the U.S. National Security Agency ("NSA") and Cybersecurity & Infrastructure Agency ("CISA") issued a joint publication titled, *Use Secure Cloud Identity and Access Management Practices.* The publication warned, "[a]s organizations continue to move to using cloud environments, these environments are becoming increasingly valuable targets for malicious cyber actors[.]"[44] The publication made numerous recommendations relevant to MFA, rotating credentials, and restricting allow lists to ensure only necessary privileges are granted to users:

> a. **Multifactor authentication.** Single-factor authentication (e.g., password or PIN only) based account access is susceptible to credential theft, forgery, and reuse across multiple systems. Cloud accounts are generally globally accessible; thus they are more susceptible to certain types of single-factor authentication weaknesses. Multifactor authentication (MFA) boosts account security, better resisting compromise by enhancing user verification methods. MFA requires two or more factors for login: something the user knows, has, or is. Typically this is implemented using a password and a second factor usually based on a randomly seeded numeric token, a biometric option (such as a fingerprint or facial recognition), or a physical token (unique hardware-based identifier: smartcard, Common Access Card, etc.).
>
> b. Periodically audit IAM configurations to confirm only necessary privileges are granted to users. Many CSPs [Cloud Service Providers] offer services that will track unused privileges to help admins tailor accounts to the least privileges users need to accomplish their day-to-day responsibilities.

[43] https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/11/cloud-computing-rfi-what-we-heard-learned (last visited Jan. 13, 2026).
[44] See https://media.defense.gov/2024/Mar/07/2003407860/-1/-1/0/CSI-CloudTop10-Mitigation-Strategies.PDF (last visited Jan. 14, 2026).

54. Also in March 2024, NSA separately issued a publication titled, *NSA's Top Ten Cloud Security Mitigation Strategies.* The publication emphasized the importance of MFA, credential rotation, and restricted allow lists as follows for customers using cloud data services as follows:[45]

> Proper identity and access management (IAM) are critical to securing cloud resources. Malicious actors can compromise accounts using phishing techniques, exposed credentials, or weak authentication practices to gain initial access into cloud tenants. They can also exploit overly broad access control policies to penetrate further into the environment, gaining access to sensitive resources. To prevent this, cloud users should use secure authentication methods such as phishing-resistant multifactor authentication (MFA) and properly managed temporary credentials. Access control policies should be carefully configured to ensure users are granted the least privileges necessary. Separation of duties should be implemented to protect especially sensitive operations and resources.

ii. Industry Standards

55. The PCI Data Security Council issued an April 2018 supplement to the PCI DSS, titled Cloud Computing Guidelines.[46] The PCI Cloud Computing Guidelines again emphasize the importance of MFA, providing: "PCI DSS Requirement 8.2.2 requires multi-factor authentication for all remote network access to the CDE [cardholder data environment], and when public cloud services are part of a Customer's CDE, all such access will be considered remote access and will require multi-factor authentication.

56. The Center for Internet Security ("CIS") is a nonprofit organization that develops globally recognized best practices for securing IT systems and data. In March 2022, CIS issued a publication entitled CIS Controls Cloud Companion Guide that provided guidance on security best

[45] *Id.*
[46] https://listings.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf (last visited Jan. 13, 2026).

practices for customers using cloud services. The guidance made the following recommendations emphasizing the importance of MFA and revoking access to stale credentials:

> a. Disable Dormant Accounts. Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.
>
> b. Establish an Access-Revoking Process. Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.
>
> c. Require MFA for Administrative Access. Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.

57. ISO/IEC 27017 is an international standard that "provides controls and implementation guidance for … cloud service customers."[47] Control 9.2.3 specifically highlights that cloud service customers (like Louis Vuitton) should use MFA as follows:

> The cloud service customer should use sufficient authentication techniques (e.g., multi-factor authentication) for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service according to the identified risks.

V. DEFENDANT ACQUIRES, COLLECTS, AND STORES PLAINTIFF'S AND CLASS MEMBERS' PRIVATE INFORMATION

58. Defendant acquires, collects, and stores a significant amount of PII belonging to Plaintiff and Class Members.

59. As a condition of utilizing or purchasing Louis Vuitton's products and services and/or their employment with Louis Vuitton, Plaintiff and Class Members were required to entrust their highly sensitive PII to Louis Vuitton.

[47] https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27017:ed-1:v1:en (last visited Jan. 14, 2026).

60. By obtaining, collecting, and using Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

61. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and would not have entrusted their PII to Defendant absent a commitment to safeguard that information.

62. Upon information and belief, Defendant promised, while collecting PII from Plaintiff and Class Members, to provide confidentiality and adequate security for their data through its applicable privacy policies and through other disclosures in compliance with statutory privacy requirements.

63. Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use their PII for business purposes only, and to make only authorized disclosures of their PII. The Data Breach occurred because Defendant failed to honor its commitments.

VI. VALUE OF PRIVATE INFORMATION

64. The FTC defines "identity theft" as "a fraud committed or attempted using the identifying information of another person without authority."[48] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number,

[48] 17 C.F.R. § 248.201 (2013).

alien registration number, government passport number, employer or taxpayer identification number."[49]

65. The PII of individuals remains of high value to criminals, as evidenced by the prices paid for PII on the dark web. Numerous sources cite dark-web pricing for stolen identity credentials.[50]

66. The PII compromised in the Data Breach is significantly more valuable than the loss of, for example, payment card information at the point of sale in a retailer data breach because, there, victims can cancel or close payment card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names, dates of birth, and Social Security numbers.

67. Among other forms of fraud, identity thieves can obtain driver's licenses, government benefits, medical services, and housing, and even provide false information to police.

68. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when the harm occurs versus when it is discovered and also between when the PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[51]

---

[49] *Id.*

[50] *See* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Jan. 13, 2026).

[51] *See* https://www.gao.gov/assets/gao-07-737.pdf (last visited Jan. 13, 2026).

69. When combined with other publicly available data, any PII element can be used to build full identity profiles, known as "Fullz" packages, which are frequently exploited in financial fraud schemes. "Fullz" is fraudster-speak for data that includes a victim's information, including name, address, SSN, date of birth, and more.

70. With Fullz packages, cybercriminals can cross-reference two (or more) sources of PII to marry unregulated data available elsewhere (e.g., address or phone number) to criminally stolen data to assemble shockingly accurate and complete dossiers on individuals.

71. Compromised PII, whether alone or as part of a Fullz package, is highly valuable to cybercriminals, who can use it to engage in a wide range of fraudulent activities, including committing unemployment insurance fraud, opening unauthorized financial accounts, and applying for government benefits.

72. This type of identity theft renders any compromised data—including seemingly innocuous PII, such as name and contact information—valuable. In the wrong hands, up-to-date names, addresses, phone numbers, and email addresses can be used to update, validate, and verify Fullz packages, which can then be used for nefarious purposes.

73. For example, a criminal actor can use an up-to-date Fullz package to bypass identity verification tools—which are often used in financial transactions (like loan applications), background checks, etc.—without detection. In a typical identity verification system, a user submits their PII, like their name, addresses, or date of birth. That customer-submitted PII is then cross-checked against "a trusted data set," including those from "credit bureaus, official government documents or mobile operator databases."

74. Thus, with an up-to-date Fullz package—which might include seemingly harmless information, like the identity theft victim's name and current address—a cybercriminal has the

victim's up-to-date PII, which will match the victim's information from trusted data sources, like the credit bureaus. With this information, the criminal can then successfully pass identity verification systems without raising any red flags. In this way, Fullz packages, which are made possible by up-to-date and compromised elements of PII, enable fraudsters to carry out various forms of identity theft, including taking out fraudulent loans.

75. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

VII. DEFENDANT BREACHED ITS DUTY OF CARE OWED TO PLAINTIFF AND CLASS MEMBERS RESULTING IN INJURY.

76. Plaintiff's and Class Members' PII was stored on Defendant's platforms, networks, systems or products at the time of the Data Breach.

77. Defendant owed common law duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised, accessed, stolen, or misused by unauthorized parties.

78. At the time of the Data Breach, Louis Vuitton failed to maintain reasonable data security measures and comply with FTC guidance and other relevant industry standards. These data security failings included Louis Vuitton's failures to adequately select or oversee its third-party vendor, Salesforce, to which Louis Vuitton entrusted the PII of its customers and/or employees.

79. Louis Vuitton's data security failings enabled the Data Breach. Without these basic protections, cybercriminals were able to exfiltrate Plaintiff's and Class Members' PII.

80. Louis Vuitton, through these data security failings, breached its express representations in its Privacy Policy which are detailed earlier in the complaint.

81. Alternatively, Louis Vuitton breached implied commitments to protect the PII of customers and employees, including Plaintiff and Class Members, by virtue of mandating that customers and employees provide their sensitive PII as a condition of using or purchasing the Louis Vuitton's products and services and/or being employed by Louis Vuitton.

82. Louis Vuitton's basic data security shortcomings also constitute a breach of their duty of care to protect the PII of customers and employees, including Plaintiff and Class Members.

83. Louis Vuitton's data security failings also constitute an unfair trade practice. As discussed above, the FTC's enforcement actions have established that a company's failure to maintain reasonable and appropriate data security of PII violates the FTC Act's prohibition on "unfair and deceptive acts."

84. Louis Vuitton's breach of its duty of care and engagement in unfair trade practices caused injury to Plaintiff and Class Members.

85. Louis Vuitton is liable for the injuries suffered by Plaintiff and Class Members by virtue of its role in the collection, transfer of and storage of the data of its affected customers.

86. Plaintiff and Class Members have and will continue to suffer the following forms of injury fairly traceable to the Data Breach.

87. The Data Breach's disclosures of Plaintiff's and Class Members' PII has created a substantial risk that their data will be misused. That cybercriminals now control that data demonstrates this risk.

88. Plaintiff and Class Members have and will continue to reasonably expend significant time and costs mitigating the substantial risk of data misuse. These mitigation steps

include Plaintiff and Class Members now expending time and effort to place "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

89. Plaintiff and Class Members have and may suffer lost property value of their PII when Defendant allowed their PII to fall into the hands of cybercriminals, who could—and likely will—freely sell or distribute it at any time.

90. Defendant breached its express and implied contractual commitments to Plaintiff and Class Members to protect their PII.

91. The breach of a contractual obligation constitutes an injury to Plaintiff and Class Members and provides a basis for a lawsuit to enforce the contractual terms.

92. In breaching its contractual commitments, Defendant further injured Plaintiff and Class Members by depriving them of the benefit of the bargain they had reached.

93. For example, Plaintiff and Class Members entered into agreements with Louis Vuitton based on express and implied representations that their PII would be protected—which they factored into the value of that exchange. By failing to maintain reasonable data security measures to protect that PII, Defendant deprived Plaintiff and Class Members of the benefit of the bargain by which they were owed the value of reasonable data security measures that were not provided.

94. Plaintiff and Class Members have or may have been injured by an invasion of their privacy rights. The disclosure of their PII to cybercriminals and potentially others if and when the cybercriminals disclose it on the dark web involves PII whose private nature was compromised by the Data Breach.

95. In addition, Plaintiff and Class Members have or may suffer emotional distress and anxiety resulting from the Data Breach and fear the substantial risk of identity theft and loss of privacy. Plaintiff and Class Members understand that their PII cannot now be clawed back from the dark web.

VIII. PLAINTIFF'S INDIVIDUAL EXPERIENCE

96. Ms. Winkler is a customer of Louis Vuitton who has purchased goods from Louis Vuitton's brick-and-mortar retail stores and online.

97. Upon information and belief, Ms. Winkler's PII was stolen from Louis Vuitton's systems, networks, and/or software in the Data Breach.

98. Louis Vuitton was in possession of Ms. Winkler's PII before, during, and after the Data Breach.

99. Because of the Data Breach, Ms. Winkler's confidential PII is in the hands of cybercriminals. As such, Ms. Winkler and other Class Members are at imminent risk of identity theft and fraud.

100. As a result of the Data Breach, Ms. Winkler must expend hours of her time and suffer loss of productivity addressing and attempting to ameliorate and mitigate the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that she is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

101. Ms. Winkler places significant value on the security of her PII and does not readily disclose it. Ms. Winkler has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

102. Ms. Winkler has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

103. Ms. Winkler has a continuing interest in ensuring that her PII, which, upon information and belief, remains in the possession of Louis Vuitton, is protected and safeguarded from future data breaches. Absent court intervention, Ms. Winkler's and Class Members' PII will be wholly unprotected and at risk of future data breaches.

104. Ms. Winkler suffered actual injury as a result of the unauthorized access and disclosure of her PII in the Data Breach including, but not limited to: (i) invasion of privacy; (ii) disclosure and/or theft of her PII; (iii) lost or diminished value of her PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) nominal damages; and (vi) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Louis Vuitton's possession and is subject to further unauthorized disclosures so long as Louis Vuitton fail to undertake appropriate and adequate measures to protect her PII.

105. The Data Breach has caused Ms. Winkler to suffer fear, anxiety, and stress, which has been compounded by the fact that Louis Vuitton has still not informed her of key details about the Data Breach.

IX. CLASS ACTION ALLEGATIONS

146. Plaintiff brings this action on her own behalf and on behalf of the following "Nationwide Class":

> **Nationwide Class.** All individuals residing in the United States whose PII was compromised in the Data Breach.

106. Excluded from the Class are Defendant's officers, directors, and any entity in which Defendant have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from each of the Classes are members of the judiciary to whom this case is assigned, their families and members of their staff.

107. Plaintiff reserves the right to amend or modify the definition of the Class or create additional subclasses as this case progresses.

108. **Numerosity**. The members of the Classes are so numerous that joinder of all Class Members is impracticable. Public reporting presently indicates that there are millions of customers and employees whose data was implicated in the Data Breach.

109. **Commonality**. There are questions of fact and law common to the Class, which predominate over individualized questions. These common questions of law and fact include, but are not limited to:

a. Whether Defendant had a duty to protect the PII of Plaintiff and Class Members and whether it breached that duty.

b. Whether Defendant knew or should have known that its data security practices were deficient.

c. Whether Defendant's data security systems were consistent with industry standards before the Data Breach.

d. Whether Plaintiff and Class Members are entitled to actual damages, punitive damages, treble damages, statutory damages, nominal damages, and/or injunctive relief.

110. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Members', was compromised in the Data Breach.

111. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Class Members. Plaintiff's Counsel are competent and experienced in litigating class actions, including data-breach class actions specifically.

112. **Predominance**. Defendant engaged in a common course of conduct toward Plaintiff and Class Members, whose data was stored on the same Louis Vuitton software and products and was unlawfully accessed in the same manner. The common issues arising from Defendant's conduct affecting Class Members predominate over any individualized issues. Adjudication of these common issues in a single action will advance judicial economy.

113. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the claims of the Class. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find the cost of litigating their individual claims to be prohibitively high and therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications as to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects each Class Member's rights.

114. Class certification is also appropriate under Rules 23(b)(1), (b)(2), and/or (c)(4) because:

- The prosecution of separate actions by individual member of the Class would create a risk of inconsistent or varying adjudications establishing incompatible standards of conduct for Defendant.

- The prosecution of separate actions by individual Class members would create a risk of adjudications that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests.

- Defendant have acted or refused to act on grounds generally applicable to the Class, making injunctive and corresponding declarative relief appropriate with respect to the classes as a whole; and

- The claims of Class members are comprise of common issues whose resolution in a class trial would materially advance this litigation.

115. Finally, all members of the proposed Class are readily ascertainable. Defendant have access to the names and contact information of all Class Members affected by the Data Breach.

X. CAUSES OF ACTION

A. Count I: Negligence (On behalf of the Plaintiff and Class Members against Defendant Louis Vuitton)

116. Plaintiff repeats and re-alleges the factual allegations above as if fully set forth herein.

117. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, and deleting their PII in its possession from being compromised, stolen, or misused by unauthorized persons.

118. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard their PII.

119. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if their PII was wrongfully disclosed.

120. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Plaintiff and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft.

121. Specifically, this duty included, among other things: (a) implementing industry standard data security safeguards to protect the PII of Plaintiff and Class Members; (b)

maintaining, testing, and monitoring Defendant's security systems to ensure that PII was adequately secured and protected; (c) implementing intrusion detection systems and timely notifying customers of suspicious intrusions; (d) ensuring any third-party software products to which it entrusted Plaintiff's and Class Members' PII were adequately and reasonably secure and not vulnerable to exploitation; and (e) adequately notifying Plaintiff and Class Members about the types of data that were compromised in the Data Breach.

122. Defendant's duties to use reasonable care arose from several sources, including those set out below.

123. Defendant had a duty to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

124. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Defendant stored valuable PII that is routinely targeted by cybercriminals. Plaintiff and Class Members were the foreseeable and probable victims of any breach resulting from Defendant's inadequate data security practices.

125. Defendant further assumed a duty of reasonable care in making representations in marketing materials and their respective Privacy Policies concerning data security.

126. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

127. Defendant had and continue to have a duty to adequately disclose that the PII of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice

was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

128. Defendant breached its duty owed to Plaintiff and Class Members by failing to maintain adequate data security practices that conformed with industry standards and were therefore negligent. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to adequately train their employees to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Plaintiff's and Class Members' PII;

e. Failing to detect in a timely manner that Plaintiff's and Class Members' PII had been compromised;

f. Failing to remove Plaintiff's and Class Members' PII it was no longer required to retain pursuant to regulations;

g. Failing to timely and adequately notify Plaintiff and Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to ensure any third party vendor or software it used were adequately and reasonably secure to protect the PII Plaintiff and Class Members entrusted to Defendant.

129. But for Defendant's negligence, the PII of Plaintiff and Class Members would not have been stolen by cybercriminals in the Data Breach.

130. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained

and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

131. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

132. The harm that occurred because of the Data Breach is the type of harm the FTC Act was intended to guard against.

133. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

134. The FTC has pursued enforcement actions against businesses, which, because they failed to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

135. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly considering Defendant's inadequate security practices.

136. Plaintiff and Class Members were the foreseeable and probable victims of any consequences of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and Class Members, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on its systems.

137. It was therefore foreseeable that failing to adequately safeguard Plaintiff's and Class Members' PII would result in one or more types of injuries to Class Members.

138. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiff's and Class Members' PII and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The PII of Plaintiff and Class Members was lost

and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

139. As a direct and proximate result of Defendant's breach of its duties, Plaintiff and Class Members have suffered injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of their PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (vii) nominal damages; and (viii) the continued and certainly increased risk to their PII, which: remains (a) unencrypted and available for unauthorized third parties to access and abuse; and (b) backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII.

140. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

141. Plaintiff and Class Members had no ability to protect their PII that was in, and remains in, Defendant's possession.

142. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members because of the Data Breach.

143. Defendant's duty extended to protecting Plaintiff and Class Members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the

actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized a specific duty to reasonably safeguard PII.

144. Defendant has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

145. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

B. Count II: Breach of Implied Contract
(On behalf of Plaintiff and the Class Members against Defendant Louis Vuitton)

146. Plaintiff repeats and re-alleges the factual allegations above as if fully set forth herein.

147. As a condition of using or purchasing Louis Vuitton's products and services and/or employment with Louis Vuitton, it required Plaintiff and Class Members to provide them with their PII.

148. In mandating that Plaintiff and Class Members provide their PII, Louis Vuitton implied an assent to safeguard and protect their PII. In so doing, Plaintiff and Class Members entered into implied contracts with Louis Vuitton by which it agreed to safeguard and protect their PII, to keep it secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

149. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Louis Vuitton's data security practices complied with relevant laws and regulations and were consistent with industry standards.

150. Implicit in the agreement between Plaintiff and Class Members, on the one hand, and Louis Vuitton, on the other, was that in providing PII, Louis Vuitton were obligated to: (a) use such PII for business purposes only; (b) take reasonable steps to safeguard that PII; (c) prevent unauthorized disclosures of the PII; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII; (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses; and (f) retain the PII only under conditions that kept it secure and confidential.

151. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Louis Vuitton, on the other, is demonstrated by their conduct and course of dealing.

152. Louis Vuitton solicited, offered, and invited Plaintiff and Class Members to provide their PII as part of Louis Vuitton's regular business practices. Plaintiff and Class Members accepted Louis Vuitton's offers and provided their PII to them.

153. In accepting the PII of Plaintiff and Class Members, Louis Vuitton understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

154. Plaintiff and Class Members would not have provided their PII to Louis Vuitton had they known that they would not safeguard their PII as promised.

155. Plaintiff and Class Members fully performed their obligations under their implied contracts with Louis Vuitton.

156. Louis Vuitton breached its implied contracts with Plaintiff and Class Members by failing to safeguard their PII.

157. At all relevant times, Louis Vuitton promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would disclose PII only under certain circumstances, none of which relate to the Data Breach.

158. Louis Vuitton further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

159. As a direct and proximate result of Louis Vuitton's breach of implied contract, Plaintiff and Class Members have suffered injuries in fact including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of their PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (vii) nominal damages; and (viii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Louis Vuitton's possession and is subject to further unauthorized disclosures so long as they fail to undertake appropriate and adequate measures to protect their PII.

160. As a direct and proximate result of Louis Vuitton's breach of implied contract, Plaintiff and Class Members are entitled to damages, including compensatory damages, punitive damages, and/or nominal damages, in an amount to be proven at trial.

C. Count III: Unjust Enrichment (On behalf of Plaintiff and Class Members against Defendant Louis Vuitton)

161. Plaintiff repeats and re-alleges the factual allegations above as if fully set forth herein.

162. Plaintiff brings this Count in the alternative to Count II above with respect to Louis Vuitton.

163. Upon information and belief, Defendant funds any data security measures it implements entirely from its general revenues, including from money it makes (including that supplied by contractual payments directly or indirectly by Plaintiff and Class Members) based upon representations of protecting PII.

164. Thus, there is a direct nexus between money paid to Defendant and the requirement that Defendant keep PII confidential and protected.

165. Plaintiff and Class Members paid Defendant a certain sum of money, which was used to fund any data security measures implemented by Defendant.

166. As such, a portion of the payments made by Plaintiff and Class Members (or made on their behalf) is to be allocated to and used to provide a reasonable and adequate level of data security, the amount of which is known to Defendant.

167. Protecting PII is integral to Defendant's businesses. Without PII, Defendant would be unable to provide the business services which comprise Defendant's core businesses.

168. Plaintiff's and Class Members' PII has monetary value. Thus, Plaintiff and Class Members conferred a monetary benefit on Defendant.

169. Defendant collected and stored the PII provided by Plaintiff and Class Members to Defendant. In exchange, Plaintiff and Class Members should have received from Defendant the services that comprise Defendant's businesses and should have had the PII protected with adequate data security.

170. Defendant knew that Plaintiff and Class Members conferred a benefit upon them and accepted and retained that benefit by accepting and retaining the PII entrusted to them. Defendant profited from the PII and used the PII for business purposes.

171. Defendant failed to secure the PII and, therefore, did not fully compensate Plaintiff and Class Members for the value that the PII provided.

172. Had Plaintiff and Class Members known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure the PII, they would not have entrusted the PII to Defendant or obtained services from Defendant.

173. Plaintiff and Class Members have no adequate remedy at law.

174. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure the PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by using cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decisions to prioritize its own profits over the requisite data security and the safety of Plaintiff's and Class Members' PII.

175. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

176. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of their PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data

Breach; (vi) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (vii) nominal damages; and (viii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII.

177. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiff and Class Members may seek restitution or compensation.

178. Because Plaintiff and Class Members may not have an adequate remedy at law against Defendant, they plead this claim for unjust enrichment in addition to or in the alternative to other claims pleaded herein.

D. Count IV: Violations of the Maryland Consumer Protection Act, Md. Code ANN., Com. Law §§ 13-301, et seq. ("MDCPA")

(On behalf of Plaintiff Winkler and Class Members residing in Maryland against both Defendant)

179. Plaintiff Winkler repeats and re-alleges the factual allegations above as if fully set forth herein.

180. Maryland Plaintiff Winkler brings this Count on her own behalf and on behalf of Class Members residing in Maryland.

181. Defendant is a "person" as defined by Md. Code, Com Law § 13-101(h).

182. Plaintiff Winkler and Class Members residing in Maryland purchased goods and services in "trade" and "commerce" as meant by Md. Code, Com. Law § 13-101(i) and § 13-303, primarily for personal, family, and/or household purposes, directly or indirectly.

183. Plaintiff Winkler and Class Members residing in Maryland are "consumers" as defined by Md. Code, Com. Law § 13-101(c).

184. Defendant advertises, offers, or sells "consumer goods" or "consumer services" as defined by Md. Code, Com. Law § 13-101(d).

185. Defendant engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of their trade and commerce in violation of Md. Code, Com. Law § 13-301, including the following:

a. Representing that their goods and services have characteristics, uses, benefits, and qualities that they do not have;

b. Representing that their goods and services are of a particular standard or quality if they are another;

c. Advertising their goods and services with intent not to sell them as advertised;

d. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members residing in Maryland's PII, which was a direct and proximate cause of the Data Breach;

e. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures after previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

f. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members residing in Maryland's PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members residing in Maryland's PII,

including by implementing and maintaining reasonable security measures;

h. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members residing in Maryland's PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

i. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members residing in Maryland's PII; and

j. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members residing in Maryland's PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

186. Had Defendant disclosed to Plaintiff Winkler and Class Members residing in Maryland that its data systems were not secure and thus were vulnerable to attack, Defendant could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiff Winker's and Class Members residing in Maryland's PII as part of the services Defendant provided and for which Plaintiff Winkler and Class Members residing in Maryland paid without advising Plaintiff Winkler and Class Members residing in Maryland that Defendant's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Class Members residing in Maryland's PII. Accordingly, Plaintiff Winkler and Class Members residing in Maryland acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

187. Defendant acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act and recklessly disregarded Plaintiff Winkler's and Class Members residing in Maryland's rights. Defendant: (1) represented in their information privacy and confidentiality policies that it was implementing reasonable security measures to protect Plaintiff

Winkler's and Class Members' sensitive personal information; and (2) failed to implement reasonable data security measures. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities that solicitor are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45.

188. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and Class Members residing in Maryland's reliance on them, Plaintiff Winkler and Class Members residing in Maryland have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant, since they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

189. Plaintiff Winkler and Class Members residing in Maryland seek all monetary and non-monetary relief allowed by law for Defendant's violations of the MDCPA, including actual damages or statutory damages, treble damages, restitution, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. An Order certifying the Class and appointing Plaintiff and their Counsel to

represent the Class;

B. Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

C. Injunctive relief, including but not limited to injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendant can provide the Court with reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to pay out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

vi. requiring Defendant to engage independent third-party security auditors and/or penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's networks is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and how to respond to a breach;

xiii. requiring Defendant to implement testing systems to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, and randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat-management program designed to appropriately monitor Defendant's information networks for internal and external threats and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face because of the loss of their confidential PII to unauthorized third parties as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: January 27, 2026

Respectfully submitted,

By: /s/ Steven M. Nathan

Steven M. Nathan (State Bar No. 2156289)
Renner K. Walker (State Bar No. 5588330)
Gisela Rosa (*pro hac vice* forthcoming)
HAUSFELD LLP
33 Whitehall Street
Fourteenth Floor
New York, NY 10004
Telephone: (646) 357-1100
Email: snathan@hausfeld.com
Email: rwalker@hausfeld.com
Email: zrosa@hausfeld.com

James J. Pizzirusso (*pro hac vice* forthcoming)
Nicholas U. Murphy (*pro hac vice* forthcoming)
HAUSFELD LLP
1201 17th Street, NW
Suite 600
Washington, DC 20036
Telephone: (202) 540-7200
Email: jpizirusso@hausfeld.com
Email: nmurphy@hausfeld.com

Dena C. Sharp (*pro hac vice* forthcoming)
Adam E. Polk (*pro hac vice* forthcoming)
GIRARD SHARP LLP
601 California Street
Suite 1400
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
Email: dsharp@girardsharp.com
Email: apolk@girardsharp.com

Jason L. Lichtman (State Bar No. 4966107)
Sean A. Petterson (State Bar No. 5412663)
LIEFF CABRASER HEIMANN & BERNSTEIN LLP
250 Hudson Street, 8th Floor
New York, New York 10013
Telephone: (212) 355-9500
Email: jlichtman@lchb.com
Email: spetterson@lchb.com

Counsel for Plaintiff